修 士 学 位 論 文

論文題名
楕円曲線のねじれ部分群を計算するアルゴリズムについて

指導教員　内田　幸寛　准教授
2020 年 1 月 10 日　提出

首都大学東京　大学院
理学研究科　数理科学専攻
学修番号　18843403

氏名　石川　岳

目次

1 概要

本研究では楕円曲線のねじれ部分群を計算するアルゴリズムについて考察する.

K を代数体, $\mathcal{O}_K$ を K の整数環とする. K 上の楕円曲線 E を方程式

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in K)$$

の解の集合と定義する (ただし, E は非特異). この方程式は適当な変数変換を行うことで, Weierstrass 型楕円曲線 $y^2 = x^3 + Ax + B$ $(A, B \in \mathcal{O}_K, 4A^3 + 27B^2 \neq 0)$ へと変形できる.

ここで代数体上の楕円曲線に関する以下のような定理が存在する.

定理 1.1 (Mordell-Weil)**.** 代数体 K 上の楕円曲線 E に対し, E の K-有理点の群 $E(K)$ は有限生成アーベル群である.

ただし, O を無限遠点として,

$$E(K) = \{P = (x, y) \in K \times K \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

とする. この定理から, $E(K)$ は有限なねじれ部分群 $E(K)_{\mathrm{tor}}$ を持つことが分かる. 与えられた楕円曲線 E に対して, この $E(K)_{\mathrm{tor}}$ を求めるアルゴリズムは等分多項式の因数分解を用いる方法などが知られている. また $K = \mathbb{Q}$ の場合, Doud のアルゴリズムや Lutz-Nagell の定理を用いた方法などでも楕円曲線のねじれ部分群を求めることができる. この中で, Doud のアルゴリズムについては, そのアルゴリズムを拡張することで, 一般の代数体 K 上の楕円曲線のねじれ部分群も求めることが可能であるかは知られていない.

本研究は K を虚 2 次体に制限した場合, Doud のアルゴリズムを拡張することで, $E(K)_{\mathrm{tor}}$ を計算することが可能であることを示している. また, 虚 2 次体上の楕円曲線のねじれ部分群を求めるアルゴリズムを具体的に構成することで, その計算時間について, 実際に等分多項式の因数分解を用いたアルゴリズムとの比較を行った.

本論文の構成は以下の通りである. 第 2 章では, 有理数体上の楕円曲線のねじれ部分群を計算する Doud のアルゴリズムについて述べる. 第 3 章では, Doud のアルゴリズムを構成する際に用いた定理を虚 2 次体へ拡張した場合の定理を与える. 第 4 章では, 本研究の主結果として, 虚 2 次体上の楕円曲線のねじれ部分群を求めるアルゴリズムを与え, その計算量についての考察と, 等分多項式の因数分解を用いたアルゴリズムと比較した数値実験の結果を載せる. 第 5 章では, その結果についての考察を述べる.

2 Doud のアルゴリズム

本研究では Doud のアルゴリズムを虚 2 次体へ拡張するが, まず Doud のアルゴリズムについて説明する. 詳しくは Doud [4] を参照せよ.

2.1 主要な 3 つの定理

Doud のアルゴリズムで用いる 3 つの定理を述べる.

定理 2.1 (Mazur)**.** 任意の $\mathbb{Q}$ 上の楕円曲線のねじれ部分群は, $\mathbb{Z}/n\mathbb{Z}$ $(1 \leq n \leq 10, n = 12)$, または $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ $(1 \leq n \leq 4)$ のいずれかに同型である.

証明. Mazur [9], [10] を参照せよ. □

定理 2.2 (Lutz-Nagell)**.** 任意の $\mathbb{Z}$ 上の楕円曲線 $E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ $(a_i \in \mathbb{Z})$ に対して, 以下が成り立つ.

- 点 $P = (x, y)$ が $E(\mathbb{Q})$ のねじれ点ならば $4x \in \mathbb{Z}$ かつ $8y \in \mathbb{Z}$ である.
- 点 $P = (x, y)$ がねじれ点で, E が Weierstrass 型楕円曲線 $y^2 = x^3 + Ax + B$ $(A,\ B \in \mathbb{Z})$ ならば $x, y \in \mathbb{Z}$. さらに $y = 0$ または $y^2 \mid 4A^3 + 27B^2$ である.

証明. Silverman [13, Corollary 7.2, p. 221] を参照せよ. □

素数 p に対して $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ とする. また $E(\mathbb{F}_p)$ を $\mathbb{F}_p$ 上の楕円曲線の $\mathbb{F}_p$-有理点の集合とする.

定理 2.3. E を $y^2 = x^3 + Ax + B$ $(A, B \in \mathbb{Z})$ の形で与えられる楕円曲線とする. p を E の判別式を割り切らない奇素数とすると, $E(\mathbb{Q})_{\mathrm{tor}}$ から $E(\mathbb{F}_p)$ への単射準同型が存在する.

証明. Silverman [13, Propositon 3.1, p. 176] を参照せよ. □

2.2 楕円曲線に対する解析的アプローチ

この節では, 楕円曲線に対する Weierstrass の $\wp$ 関数の定義とその性質について述べる.
$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ とする (ただし, $\omega_1, \omega_2 \in \mathbb{C}$ は $\mathbb{R}$ 上線形独立とする). L を格子と呼ぶ. また, L に対して,

$$F = \{a_1\omega_1 + a_2\omega_2 \mid 0 \leq a_i < 1, i = 1, 2\}$$

を L の基本平行四辺形という.

定理 2.4.

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

とおく. $\wp(z)$ を Weierstrass の $\wp$ 関数という. $\wp$ 関数は以下を満たす.

1. $\wp(z)$ は $\mathbb{C} \setminus L$ におけるコンパクト集合上で, 絶対かつ一様収束する.
2. $\wp(z)$ は $\mathbb{C}$ における有理型関数かつ L の各点に 2 位の極を持つ.
3. 任意の $z \in \mathbb{C}$ に対し, $\wp(-z) = \wp(z)$.
4. 任意の $\omega \in L$ に対し, $\wp(z + \omega) = \wp(z)$.

証明. Washington [14, Theorem 9.3] を参照せよ. □

定義 2.1. $k \geq 3$ に対して,

$$G_k = G_k(L) = \sum_{\omega \in L, \omega \neq 0} \omega^{-k}$$

と定義する. G_k をアイゼンシュタイン級数と呼ぶ.
これは, 絶対収束する. また k が奇数のとき, $G_k = 0$.

定理 2.5. $\wp(z)$ を格子 L に対する Weierstrass の $\wp$ 関数とする.

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

証明. Washington [14, Theorem 9.8] を参照せよ. □

いま,

$$g_2 = 60G_2$$
$$g_3 = 140G_4$$

と表記することにすると, 点 $(\wp(z), \wp'(z))$ は,

$$E : y^2 = 4x^3 - g_2x - g_3$$

という曲線上の点である. なお, この曲線の判別式は $16(g_2^3 - 27g_3^2)$ であるが, $g_2^3 - 27g_3^2 \neq 0$ であることが知られているため, 曲線 E は楕円曲線となる. 従って, $z \in \mathbb{C}$ から楕円曲線上の点 $(\wp(z), \wp'(z))$ への写像を考えることができる. ただし, $\wp(z), \wp'(z)$ は $z \bmod L$ に依存するため, 実際には $\mathbb{C}/L$ から $E(\mathbb{C})$ への写像を考える.

定理 2.6. L を格子, E を楕円曲線 $y^2 = 4x^3 - g_2x - g_3$ とする. 写像

$$\begin{aligned}\Psi : \mathbb{C}/L &\to E(\mathbb{C}) \\ z &\mapsto (\wp(z), \wp'(z)) \\ 0 &\mapsto O\end{aligned}$$

は群同型である.

証明. Washington [14, Theorem 9.10] を参照せよ. □

この定理により, $E(K)$ のねじれ点を求める問題を, $\mathbb{C}/L$ におけるねじれ点を見つけ, その点の像が $E(K)$ に含まれるかという問題に置き換えることができる.

ここで, 与えられたある $\mathbb{C}$ 上の楕円曲線に対して, 格子 L を定義する ω_1, ω_2 は, 楕円曲線の方程式の右辺の根を求める, かつ AGM アルゴリズムを適用することで得ることができる. また, この AGM アルゴリズムは 2 次収束するが, 後に述べる本研究におけるアルゴリズムは定理 2.7 のような 1 次収束する級数を含む. 従って, ω_1, ω_2 の計算はアルゴリズム全体の計算量に影響しない (詳しくは Cremona, Thongjunthug [3] を参照せよ).

さらに, $\wp$ 関数を具体的に計算するための定理についても, ここで述べる.

定理 2.7. $z \in \mathbb{C}, u = e^{2\pi iz/\omega_1}, \tau = \omega_2/\omega_1 (\mathrm{Im}(\tau) > 0$ とする$), q = e^{2\pi i\tau}$ とおく.

$$\wp(z) = \left(\frac{2\pi i}{\omega_1}\right)^2 \left(\frac{1}{12} + \frac{u}{(1-u)^2} + \sum_{n=1}^{\infty} q^n \left(\frac{u}{(1-q^n u)^2} + \frac{u}{(q^n - u)^2} - \frac{2}{(1-q^n)^2}\right)\right)$$

証明. Washington [14, Theorem 9.35] を参照せよ. □

2.3 Doud のアルゴリズムの概略

前節の定理を用いて, 有理数体上の楕円曲線のねじれ部分群を求める Doud のアルゴリズムの概略を述べる. $E : y^2 = x^3 + Ax + B$ $(A, B \in \mathbb{Z})$ を楕円曲線とする. AGM アルゴリズムを用いることにより, 与えられた楕円曲線 E に対する格子 $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ を得る. また定理 2.3 より, いくつかの E の判別式を割り切らない素数 p に対して $\#E(\mathbb{F}_p)$ を計算することで, $\#E(\mathbb{Q})_{\mathrm{tor}}$ の上界 b を得る. この b を割り切る, かつ

Mazur の定理に当てはまるような n について大きい方から順番に試していく. 具体的には, まず $\mathbb{C}/L$ の n-ねじれ点 z に対し, $(\wp(z), \wp'(z))$ を計算する. ここで, $\mathbb{Q}$ 上の楕円曲線を考えているので, $\mathbb{C}/L$ の n-ねじれ点は $\omega_1/n, \omega_1/n + \omega_2/2, \omega_1/n + \omega_1/2 + \omega_2/2$ のいずれかである. Lutz-Nagell の定理より $\wp(z), \wp'(z)$ に近い整数を座標とする点を P とし, $P \in E(\mathbb{Q})$ かつ $nP = O$ となるかを確認する. この条件を点 P が満たせば, 点 P が $E(\mathbb{Q})_{\mathrm{tor}}$ の生成元となり, $E(\mathbb{Q})_{\mathrm{tor}}$ と同型な群を決定できる.

3 定理の拡張

この章では Doud のアルゴリズムを虚 2 次体上へ拡張するために, Mazur の定理, Lutz-Nagell の定理, 定理 2.3, それぞれを 2 次体の場合に拡張したものを紹介する.

K を 2 次体とする.

定理 3.1. 任意の K 上の楕円曲線のねじれ部分群は, 以下のいずれかに同型である.

$\mathbb{Z}/m\mathbb{Z}$	$(1 \le m \le 16, m = 18)$	
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$	$(1 \le m \le 6)$	
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z}$	$(m = 1, 2)$	ただし $K = \mathbb{Q}(\sqrt{-3})$ のときのみ
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$		ただし $K = \mathbb{Q}(\sqrt{-1})$ のときのみ

証明. Kenku, Momose [7], Kamienny [5] を参照せよ. □

ここで $\mathcal{O}_K$ を K の整数環とする. $\mathcal{O}_K$ はデデキント環だから零でない素イデアルは極大イデアルである. $\mathcal{O}_K$ をある零でない素イデアル $\mathfrak{p}$ で局所化した環を $R = S^{-1}\mathcal{O}_K$ $(S = \mathcal{O}_K \setminus \mathfrak{p})$ とすると, R は離散付値環であるから単項イデアル整域である. R のある素元 π において, $\alpha \in K$ に対して, $\alpha = \pi^r u$ $(u \in R^*)$ とかけるとき, $r = \mathrm{ord}_\pi(\alpha)$ とおく. また, E を

$$E : y^2 = x^3 + Ax + B \quad (A, B \in \mathcal{O}_K)$$

の形で与えられる楕円曲線とする.

以下, Lutz-Nagell の定理を 2 次体の場合へ拡張した定理について, Lang [8] に従って述べる.

補題 3.1. $n \in \mathbb{Z}_{\ge 1}$ を素数のベキでないとし, $P = (x, y) \in E(K)$ を位数がちょうど n である点とする. すると

$$x \in \mathcal{O}_K.$$

証明. Lang [8, Theorem 2.1, p. 55] を参照せよ. □

補題 3.2. 素数 p に対して, $P = (x, y) \in E(K)$ を位数 p^m $(m \in \mathbb{Z}_{\ge 1})$ のねじれ点とする. R の素元 π が p を割り切ると仮定し, e を π の分岐指数とおく. すると,

$$\mathrm{ord}_\pi(x) \ge -2r, \quad \mathrm{ord}_\pi(y) \ge -3r. \quad \left(\text{ただし}, r = \left[\frac{e}{4}\right]\right)$$

$[\cdot]$ はガウス記号を表す.

証明. Lang [8, Theorem 1.3, p. 51] を参照せよ. □

補題 3.3. $P=(x,y)\in E(K)$ に対して, $2P=(x_2,y_2)$ とおく. E の判別式を $\Delta_0=4A^3+27B^2$ とすると,

$$y^2(4x_2(3x^2+4A)-3x^3+5Ax+27B)=\Delta_0.$$

特に, $P,2P$ が整数点ならば $y^2\mid\Delta_0$.

証明. Lang [8, Theorem 1.4, p. 52] を参照せよ. □

これらの補題を用いて, Lutz-Nagell の定理の 2 次体の場合についての定理を述べる. なお, この定理は補題から直ちに従うが, 記載されている文献を見つけられないため, 以下で証明を与える.

定理 3.2. $P=(x,y)\in E(K)_{\mathrm{tor}}$ とすると,

$$x,y\in\mathcal{O}_K.$$

さらに, $y=0$ または $y^2\mid\Delta_0$.

証明. 補題 3.1 より, P の位数が素数のベキでないとき, $x,y\in\mathcal{O}_K$. P の位数を p^m (p は素数) とする. いま K は 2 次体だから, p を割り切る任意の R の素元 π に対して, $e\leq 2<4$ である. 従って, 補題 3.2 より p を割り切る全ての R の素元 π について, $r=0$ を得る. よって, $x,y\in\mathcal{O}_K$.
また, P がねじれ点のとき, $2P$ もねじれ点だから, $P,2P$ は整数点である. 補題 3.3 より, $y^2\mid\Delta_0$. □

R の素元 π による還元写像を

$$\begin{aligned} R&\to k=R/\pi R\\ t&\mapsto\tilde{t}\end{aligned}$$

と定義する. このとき, $\mathcal{O}_K/\mathfrak{p}$ と $R/\pi R$ は自然な同型になる. また楕円曲線 E に対して, 曲線 $\tilde{E}$ を

$$\tilde{E}:y^2=x^3+\tilde{A}x+\tilde{B}$$

とおく.

定理 3.3. R の素元 π に対して, 曲線 $\tilde{E}$ が非特異であるとすると, 写像

$$\begin{aligned} \Psi:E(K)_{\mathrm{tor}}&\to\tilde{E}(k)\\ P=(x,y)&\mapsto\tilde{P}=(\tilde{x},\tilde{y})\\ O&\mapsto\tilde{O}\end{aligned}$$

が存在し, Ψ は単射かつ群準同型である.

証明. 定理 3.2 より, 上記のように定義できる写像 Ψ が存在することが分かる. Ψ が群準同型であることはよく知られている. また単射性については定義より明らかである. □

注意 1. 定理 3.2, 定理 3.3 では, K は 2 次体であり, 楕円曲線を Weierstrass 型として考えている. しかし, 一般の代数体 K 上の楕円曲線

$$E:y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\quad(a_i\in\mathcal{O}_K)$$

に対しては, 以下のような定理が存在する. この定理は, 本質的には Cassels が証明を与えた ([1] を参照せよ). ここで, R は代数体 K の整数環 $\mathcal{O}_K$ をある零でない素イデアル $\mathfrak{p}$ で局所化した環, $k=R/\pi R$ とする.

定理 3.4. $P=(x,y)\in E(K)$ を位数 $m\in\mathbb{Z}_{\geq 2}$ のねじれ点とする.

1. m が素数のベキでないとき,
$$x,y\in\mathcal{O}_K.$$
2. 素数 p に対して, $m=p^s$ とする. また R の素元 π が p を割り切ると仮定し, e を π の分岐指数とおく. すると,
$$\mathrm{ord}_\pi(x)\geq -2r,\quad \mathrm{ord}_\pi(y)\geq -3r.\quad \left(\text{ただし}, r=\left[\frac{e}{\phi(p^s)}\right]\right)$$
ϕ はオイラー関数である. 特に, $e<p-1$ ならば $\mathrm{ord}_\pi(x)\geq 0, \mathrm{ord}_\pi(y)\geq 0$.

証明. Silverman [13, Theorem 7.1, p. 240] を参照せよ. □

定理 3.4 から以下の定理が導かれる.

定理 3.5. 素数 p に対して R の素元 π が $\mathrm{ord}_\pi(p)=e<p-1$ を満たすと仮定する. 楕円曲線 E を素元 π で還元した曲線 $\tilde{E}$ が非特異であるとき, 写像
$$\begin{aligned}\Psi : E(K)_{\mathrm{tor}} &\to \tilde{E}(k)\\ P=(x,y) &\mapsto \tilde{P}=(\tilde{x},\tilde{y})\\ O &\mapsto \tilde{O}\end{aligned}$$
が存在し, Ψ は単射かつ群準同型である.

定理 3.4 は, 代数体上の楕円曲線のねじれ点が一般に整数点でないことを示している. このことは, Doud のアルゴリズムを一般の代数体上へ拡張することを困難にしている要因の 1 つである.

4 主結果

4.1 アルゴリズムの構成

この節では, 前章の定理を用いて, 虚 2 次体 $K=\mathbb{Q}(\sqrt{-D})$, $D\in\mathbb{Z}_{\geq 1}$ 上の楕円曲線のねじれ部分群を求めるアルゴリズムを構成する. なお $\mathcal{O}_K$ と R については前章で定義した通りである.

予め $2\leq n\leq 16$ かつ $n=18$ に対して, $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ の部分群で $\mathbb{Z}/n\mathbb{Z}$ と同型な群 H の生成元のリストを計算しておく.

与えられた K 上の楕円曲線に対して, 適当な変数変換を用いて
$$E: y^2=x^3+Ax+B\quad (A,B\in\mathcal{O}_K)$$
とする. 後の節で述べるように, 計算精度としては $\log(3^4\max(|A^3|,|B^2|))+2$ ビットで十分である. まず K から $\mathbb{C}$ への埋め込みを定め, AGM アルゴリズムを用いて楕円曲線 E に対する周期 ω_1,ω_2 を計算する. 次に, 曲線 $\tilde{E}$ が非特異となるような還元写像を与える R のいくつかの素元 π に対して (本研究では 20 個の素元を取る), $k=R/\pi R$ として $\#\tilde{E}(k)$ を計算し, それらの最大公約数を上限値 b とする. 定理 3.3 より, $E(K)_{\mathrm{tor}}$ の位数は b の約数である.

- $b=1$ のとき：$E(K)_{\mathrm{tor}}$ と同型な群として, 自明な群を出力する.
- $4\nmid b$ のとき：以下のように場合分けをする.
  - ◆ $9\nmid b$ のとき：定理 3.1 より $E(K)_{\mathrm{tor}}$ は $\mathbb{Z}/n\mathbb{Z}$ $(1\leq n\leq 15)$ のいずれかに同型である. 従って b を割り切るような n に対して, 以下の操作を大きい方から順番に実行していく.

    [$E(K)$ の n-ねじれ点の計算]

    1. 予め計算してある $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ の部分群と同型な群 H の生成元 (s,t) $(s,t\in\mathbb{Z}/n\mathbb{Z})$ に対して, $\wp(s\omega_1/n+t\omega_2/n), \wp'(s\omega_1/n+t\omega_2/n)$ を計算する.
    2. $\wp(s\omega_1/n+t\omega_2/n), \wp'(s\omega_1/n+t\omega_2/n)/2$ に対して, それぞれの値に最も近い $\mathcal{O}_K$ の値を x,y として, 点 $P=(x,y)$ とおく. なお近い値の求め方は以下の通りである.
       - $-D\equiv 2, 3 \pmod 4$ のとき：$\wp(s\omega_1/n+t\omega_2/n)$ を実部 α, 虚部 β に分ける. K の整数環は $\mathbb{Z}[\sqrt{-D}]$ であるから, 定理 3.2 より, $x\in\mathbb{Z}[\sqrt{-D}]$. 従って $\alpha,\beta/\sqrt{D}$ を四捨五入した値をそれぞれ α',β' とおき, $x=\alpha'+\beta'\sqrt{-D}$ とする. y についても同様.
       - $-D\equiv 1 \pmod 4$ のとき：$\wp(s\omega_1/n+t\omega_2/n)$ を実部 α, 虚部 β に分ける. K の整数環は $\mathbb{Z}[(1+\sqrt{-D})/2]$ であるから, 定理 3.2 より, $x\in\mathbb{Z}[(1+\sqrt{-D})/2]$. 従って $2\alpha,(2/\sqrt{D})\beta$ を四捨五入した値をそれぞれ α',β' とおき, $x=\alpha'/2+(\beta'/2)\sqrt{-D}$ とする. y についても同様.
    3. $P\in E(K)$ かつ $nP=O$ となるかを確認する. これを満たすならば, 点 P は $E(K)_{\mathrm{tor}}$ の生成元になり, $\mathbb{Z}/n\mathbb{Z}$ を出力する.
    4. 上記の操作を部分群 H の各生成元に対して行う. 全ての生成元が条件を満たさないならば, 次の n に対して同様の操作を行う.
    5. 全ての n が条件を満たさないならば, 自明な群を出力する.

    これにより $E(K)_{\mathrm{tor}}$ と同型な群として, $\mathbb{Z}/n\mathbb{Z}$ または自明な群を得る.
  - ◆ $9\mid b$ のとき：定理 3.1 より, $D=3$ のときのみ $E(K)_{\mathrm{tor}}$ は $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3m\mathbb{Z}$ $(m=1,2)$ と同型である可能性がある. そこで $\wp(\omega_1/3), \wp'(\omega_1/3)/2, \wp(\omega_2/3), \wp'(\omega_2/3)/2$ を計算し, それぞれの値に近い $\mathcal{O}_K$ の値を x_1,y_1,x_2,y_2 とおき, $P_1=(x_1,y_1), P_2=(x_2,y_2)$ とする. いま $E(K)_{\mathrm{tor}}$ が $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3m\mathbb{Z}$ と同型ならば $P_1,P_2\in E(K)$ となるはずである.
    - $P_1,P_2\in E(K)$ かつ $D=3$ であるとき：$E(K)_{\mathrm{tor}}$ は $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3m\mathbb{Z}$ $(m=1,2)$ のいずれかに同型である. ここで楕円曲線 E の方程式の右辺 x^3+Ax+B の根の個数を l とする.
      - $l=0$ のとき：$E(K)_{\mathrm{tor}}$ は 2-ねじれ点を持たないので, $E(K)_{\mathrm{tor}}$ と同型な群として, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ を得る.
      - $l=1$ のとき：$E(K)_{\mathrm{tor}}$ は 2-ねじれ点をただ一つ持つので, $E(K)_{\mathrm{tor}}$ と同型な群として, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ を得る.
    - それ以外のとき：$E(K)_{\mathrm{tor}}$ は $\mathbb{Z}/n\mathbb{Z}$ $(1\leq n\leq 15, n=18)$ のいずれかに同型であるから, $9\nmid b$ のときと同様の操作を行う.
- $4\mid b$ のとき：以下のように場合分けをする.
  - ◆ $9\nmid b$ のとき：さらに以下のように場合分けをする.
    - $16\nmid b$ のとき：定理 3.1 より, $E(K)_{\mathrm{tor}}$ は $\mathbb{Z}/n\mathbb{Z}$ $(1\leq n\leq 15)$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}$ $(1\leq m\leq 6)$

のいずれかに同型である.

- $l=0$ のとき：$E(K)_{\mathrm{tor}}$ は 2-ねじれ点を持たないので, 奇数 n に対して, 大きい方から順番に [$E(K)$ の n-ねじれ点の計算] を実行し, $E(K)_{\mathrm{tor}}$ と同型な群として, $\mathbb{Z}/n\mathbb{Z}$ または自明な群を得る.
- $l=1$ のとき：$E(K)_{\mathrm{tor}}$ は 2-ねじれ点をただ一つ持つので, 偶数 n に対して, 大きい方から順番に [$E(K)$ の n-ねじれ点の計算] を実行し, $E(K)_{\mathrm{tor}}$ と同型な群として, $\mathbb{Z}/n\mathbb{Z}$ を得る.
- $l=3$ のとき：$E(K)_{\mathrm{tor}}$ は 2-ねじれ点を 3 つ持つので, $E(K)_{\mathrm{tor}}$ は $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}$ $(1\leq m\leq 6)$ のいずれかに同型である. 従って, $m=6,\cdots,1$ に対して $n=2m$ として順番に [$E(K)$ の n-ねじれ点の計算] を実行し, $E(K)_{\mathrm{tor}}$ と同型な群として, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}$ を得る.

∗ $16\mid b$ のとき：$\wp(\omega_1/4), \wp'(\omega_1/4)/2, \wp(\omega_2/4), \wp'(\omega_2/4)/2$ を計算し, それぞれの値に近い $\mathcal{O}_K$ の値を x_3, y_3, x_4, y_4 とおき, $P_3=(x_3,y_3), P_4=(x_4,y_4)$ とする.

- $P_3, P_4\in E(K)$ かつ $D=1$ であるとき：$E(K)_{\mathrm{tor}}$ と同型な群として, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ を得る.
- それ以外のとき：$E(K)_{\mathrm{tor}}$ は $\mathbb{Z}/n\mathbb{Z}$ $(1\leq n\leq 16)$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}$ $(1\leq m\leq 6)$ のいずれかに同型であるから, $16\nmid b$ のときと同様の操作を行う.

◆ $9\mid b$ のとき：$4\nmid b$ かつ $9\mid b$ のときと同様に $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3m\mathbb{Z}$ と同型になるかを確認する. 同型でない場合は $4\mid b$ かつ $9\nmid b$ のときと同様の操作を行う.

上記のアルゴリズムの具体例を与える.

$K=\mathbb{Q}(\sqrt{-1})$ として楕円曲線のねじれ部分群を計算する. 楕円曲線 E を

$$E: y^2=x^3-(519075+196344\sqrt{-1})x+(129864114+85934520\sqrt{-1})$$

とする. E の判別式は $4A^3+27B^2=-63347229534763008-1925671990892544\sqrt{-1}$ である. また $K=\mathbb{Q}(\sqrt{-1})$ だから $\mathcal{O}_K$ は単項イデアル整域である. 従って, この判別式が 0 にならないような還元写像を与える 20 個の素元 $\pi\in\mathcal{O}_K=\mathbb{Z}[\sqrt{-1}]$ に対して, $\#\tilde{E}(\mathcal{O}_K/\pi\mathcal{O}_K)$ を計算し, 最大公約数をとることで上限値として 7 を得る. さらに, $\log(3^4\max(|A^3|,|B^2|))+2$ ビットの計算精度で AGM アルゴリズムを用いることで, 楕円曲線 E に対する周期

$$\omega_1=0.13763846005987042124+0.0023879170433909900940\sqrt{-1}$$
$$\omega_2=-0.0081603625555070421831-0.0872113190977131105 60\sqrt{-1}$$

を得る. いま上限値は 7 であるから, $\#E(K)_{\mathrm{tor}}$ は 7 の約数であることに注意して, ω_1,ω_2 を用いて $\wp$ 関数を順番に計算すると, $\mathbb{Z}/7\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}$ の部分群と同型な群の生成元 (1, 5) に対して,

$$\wp\left(\frac{1}{7}\omega_1+\frac{5}{7}\omega_2\right)=(-159.000000\cdots)-\sqrt{-1}\times(756.000000\cdots)$$

を得る. 同様に,

$$\wp'\left(\frac{1}{7}\omega_1+\frac{5}{7}\omega_2\right)=(50544.000000\cdots)+\sqrt{-1}\times(34992.000000\cdots)$$

を得る. これらの $\wp, \wp'/2$ に近い $\mathcal{O}_K$ 上の点

$$(x, y) = (-159 - 756\sqrt{-1}, 25272 + 17496\sqrt{-1})$$

は $E(K)$ 上の点であることと, 位数が 7 であることが確かめられる. 従って, $E(K)_{\mathrm{tor}}$ の生成元は点 $(-159 - 756\sqrt{-1}, 25272 + 17496\sqrt{-1})$ であり, $E(K)_{\mathrm{tor}}$ と同型な群として, $\mathbb{Z}/7\mathbb{Z}$ を得る.

4.2 計算量の考察

この節では, 前節で構成したアルゴリズムの計算量の評価を行う. 前述のアルゴリズムにおいて最も計算時間を要する部分は, $\wp$ 関数の計算であるが, まずは, 計算する楕円曲線のねじれ点 $P = (x_1, y_1)$ の各座標の絶対値と楕円曲線上の点同士の計算時間を評価する. 楕円曲線は $y^2 = x^3 + Ax + B$ $(A, B \in \mathcal{O}_K)$ であると仮定する. 定理 3.2 より, $|y_1| \leq \Delta_0$ かつ x_1 は, $x^3 + Ax + (B - y_1^2)$ の根だから,

$$\begin{aligned} |x_1| &\leq \max(|A|, |B - y_1^2|) \\ &\leq \max(|A|, |B| + |4A^3 + 27B^2|) \\ &\leq 3^4 \max(|A^3|, |B^2|) \end{aligned}$$

となる. 従って $3^4 \max(|A^3|, |B^2|) = C$ とおくと, x_1, y_1 の絶対値は $O(C)$ で評価できる. ここで, 絶対値が $O(C)$ の値の算術演算には $O(\log^2 C)$ ビットの時間がかかる. また楕円曲線上の点同士の計算には, 有限回の楕円曲線上の群演算と各楕円曲線上の群演算に対して有限回の算術演算を要する. 従って, 本研究におけるアルゴリズムのうち, 楕円曲線上の点同士の計算時間は, $O(\log^2 C)$ である.

次に $\wp$ 関数の計算時間について評価する. 定理 2.7 より, $\wp$ 関数について

$$\wp(z) = \left(\frac{2\pi i}{\omega_1}\right)^2 \left(\frac{1}{12} + \frac{u}{(1-u)^2} + \sum_{n=1}^{\infty} q^n \left(\frac{u}{(1-q^n u)^2} + \frac{u}{(q^n - u)^2} - \frac{2}{(1-q^n)^2}\right)\right) \tag{1}$$

とかける. 実際, 格子 L に対する周期 ω_1, ω_2 を適当に変換することで, $\mathrm{Im}(\tau) > \sqrt{3}/2$ となるようにできる (Serre [12, Proposition 3, p. 82] を参照せよ). 従って $|q| \leq k$ $(k = e^{-2\pi\sqrt{3}/2} \fallingdotseq 4.33 \times 10^{-3})$ となる. さらに, z を ω_1, ω_2 に対する基本平行四辺形の中から選ぶことで, $|q| < |u| \leq 1$ とできる.

ここで点 $(\wp(z), \wp'(z))$ が楕円曲線 $y^2 = 4x^3 - g_2 x - g_3$ のねじれ点とすると, 点 $(4\wp(z), 4\wp'(z))$ は $A' = -4g_2, B' = -16g_3$ として, Weierstrass 型楕円曲線 $y^2 = x^3 + A'x + B'$ 上の点となる. 従って等式 (1) の級数の項は, 余りが $1/8$ 未満になるところまで計算すれば十分である. つまり M 項まで加えるとして, $M + 1$ 項以降の和が $1/8$ 未満であればよい. 級数の中の各分数は, $1/|q|^2$ の定数倍で上から抑えられるので, 定数 K_1 を用いて, 余りである $M + 1$ 項以降の和は $K_1 |q|^{M-2}$ で上から抑えられる. いま, この余りは $(2\pi i/\omega_1)^2$ 倍されるが, 以下の等式を用いることで上から評価できる (Chandrasekharan [2, Corollary 2, p. 69] を参照せよ).

$$\omega_1^3 = \frac{2\pi^3}{\Delta_0^{1/4}} \theta_1^2(0, \tau) \theta_2^2(0, \tau) \theta_3^2(0, \tau),$$

ただし, $q = e^{2\pi i\tau}$ として

$$\theta_1(v,\tau) = 2\sum_{n=0}^{\infty} q^{\frac{1}{8}(2n+1)^2}\cos(2n+1)\pi v,$$
$$\theta_2(v,\tau) = 1 + 2\sum_{n=1}^{\infty}(-1)^n q^{\frac{1}{2}n^2}\cos(2n\pi v),$$
$$\theta_3(v,\tau) = 1 + 2\sum_{n=1}^{\infty} q^{\frac{1}{2}n^2}\cos(2n\pi v)$$

とする. よって $\theta_1(0,\tau) = 2(q^{1/8} + q^{9/8} + q^{25/8} + \cdots), \theta_2(0,\tau) = 1 - 2q^{1/2} + 2q^{4/2} - 2q^{9/2} + \cdots, \theta_3(0,\tau) = 1 + 2q^{1/2} + 2q^{4/2} + 2q^{9/2} + \cdots$ である. また $\Delta_0 = 4A^3 + 27B^2$ である. いま $|q| \leq k$ であるから, $|\theta_2(0,\tau)| > 1/2, |\theta_3(0,\tau)| > 1/2, |\theta_1(0,\tau)| > |q|^{1/8}$ という不等式を得る. 従って,

$$|\omega_1| > \frac{\pi}{2|\Delta_0|^{1/12}}|q|^{1/12}.$$

以上より,

$$\left(\frac{2\pi}{\omega_1}\right)^2 K_1|q|^{M-2} < \frac{4\pi^2|\Delta_0|^{1/6}K_1 q^{M-2-1/6}}{(\pi/2)^2} \leq 16K_1|\Delta_0|^{1/6}k^{M-13/6}$$

が $1/8$ 未満であればよいので,

$$\begin{aligned} 16K_1|\Delta_0|^{1/6}k^{M-13/6} &< \frac{1}{8} \\ k^{M-13/6} &< \frac{1}{2^7K_1|\Delta_0|^{1/6}} \\ \left(M - \frac{13}{6}\right)\log k &< -\log(2^7K_1|\Delta_0|^{\frac{1}{6}}) \\ M &> \frac{13}{6} - \frac{1}{\log k}\left(7\log 2 + \log K_1 + \frac{1}{6}\log|\Delta_0|\right) \end{aligned}$$

となる. よって,

$$M = O(\log|\Delta_0|) = O(\log C)$$

を得る. $E(K)$ のねじれ点 P の x 座標 x_1 の絶対値は C 以下であるから, Doud [4] によると, 各項はおおよそ $2 + \log C$ 桁の精度で計算すればよい. 従って, 各項の算術演算の計算時間は $O(\log^2 C)$ である. また上記の議論から, $M = O(\log C)$ 項まで計算すればよいので, $\wp$ 関数の計算量は, $O(\log^3 C)$ である. $\wp'$ に関しても同様の結果を得ることができるかつ, 計算すべき点の個数は $O(1)$ で評価できるから, 本研究のアルゴリズムの計算時間は $O(\log^3 C)$ で評価できる.

4.3 等分多項式

この節では, 次節で計算量の比較を行うアルゴリズムに用いられる等分多項式について, 概略を述べる. 詳しくは Lang [8] を参照せよ.

アーベル群 A に対して, $A[n]$ を A の n-ねじれ点の集合とする. $n \in \mathbb{Z}_{>1}$ に対して, 以下の楕円関数 f_n が存在する.

$$f_n(z)^2 = n^2 \prod_{0 \neq u \in (\mathbb{C}/L)[n]} (\wp(z) - \wp(u)).$$

いま f_n の符号は次のように決定する.

1. n : 奇数 $\Rightarrow f_n = P_n(\wp)$, ただし P_n は次数 $(n^2-1)/2$ かつ最高次係数が n であるような多項式である.

$$f_n = n\wp^{(n^2-1)/2} + \cdots .$$

2. n : 偶数 $\Rightarrow f_n = \frac{1}{2}\wp' P_n(\wp)$, ただし P_n は次数 $(n^2-4)/2$ かつ最高次係数が n であるような多項式である.

$$f_n = \frac{n}{2}\wp'\wp^{(n^2-4)/2} + \cdots .$$

従って, f_n の $z=0$ における展開は,

$$f_n(z) = \frac{(-1)^{n+1}n}{z^{n^2-1}} + \cdots$$

となる. また f_n の根は明らかに $0 \neq u \in (\mathbb{C}/L)[n]$ である.

命題 4.1. $\wp_n(z) = \wp(nz)$ とおく.

$$\wp_n = \wp - \frac{f_{n+1}f_{n-1}}{f_n^2}.$$

証明. Lang [8, Theorem 1.1, p. 34] を参照せよ. □

さらに f_n は以下の漸化式を満たす.

命題 4.2.

$$f_{2n+1} = f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1}$$
$$\wp' f_{2n} = f_{2n}f_2 = f_n(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2)$$

証明. Lang [8, Theorem 1.3, p. 37] を参照せよ. □

ここで改めて

$$x = \wp, \quad y = \frac{1}{2}\wp', \quad A = -\frac{1}{4}g_2, \quad B = -\frac{1}{4}g_3$$

と置き換えると, 曲線

$$y^2 = x^3 + Ax + B$$

は楕円曲線になる. さらに命題 4.1 を用いると

$$f_1 = 1, \quad f_2 = 2y$$
$$f_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$
$$f_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$$

とかける. いま f_n についても

$$f_n = \psi_n(x, y)$$

と置き換える. これらの記号を用いて前述の主張をまとめると次のようにかける.

定理 4.1.

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$$
$$4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2$$

とおく.

1.
$$n(x,y) = \left(\frac{\phi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3}\right).$$

2. ϕ_n, ψ_n (n : 奇数), $\psi_n/2y$ (n : 偶数) は $\mathbb{Z}[x, A, B]$ の多項式である. 特に,
$$\phi_n(x) = x^{n^2} + \cdots$$
$$\psi_n^2(x) = n^2 x^{n^2-1} + \cdots.$$
とかける. ψ_n を等分多項式とよぶ.

定理 4.1 より, n に対する等分多項式 ψ_n を因数分解することで, 楕円曲線のねじれ点を得ることができ, 楕円曲線のねじれ部分群と同型な群を求めることができる.

4.4 数値実験

この節では, 前節で述べた等分多項式の因数分解を用いたアルゴリズム (等分多項式アルゴリズムとする) と 4.1 節の Doud のアルゴリズムを拡張したアルゴリズム (Doud の拡張アルゴリズムとする) の計算量の比較を行う.

以下, 数値実験の結果について述べる. 利用した計算機は Intel Core i5-7200U 2.70GHz のプロセッサ, メモリ 8.0GB を実装した Windows 10 Pro, 64 ビットオペレーティングシステム, ソフトウェアは Sage Math 8.8 である.

今回は $\mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ と同型であるねじれ部分群を持つ $\mathbb{Q}(\sqrt{-1})$ 上の楕円曲線に対して実験を行っている. なおそれぞれの楕円曲線の構成には, Schmitt, Zimmer [11, Theorem 6.18] を参考にした. 具体的には, $K = \mathbb{Q}(\sqrt{-1})$ として, 以下のように楕円曲線 E を構成すると, 各有限アーベル群は $E(K)_{\mathrm{tor}}$ と同型になる.

- $\mathbb{Z}/7\mathbb{Z}$: b, c をパラメータ $\alpha \in K$ を用いて
$$b = \alpha^2(\alpha - 1), \quad c = \alpha - 1$$
とおき, 楕円曲線 E を
$$E : y^2 + (1-c)xy - by = x^3 - bx^2$$
とする.
- $\mathbb{Z}/9\mathbb{Z}$: b, c をパラメータ $\alpha \in K$ を用いて
$$b = \alpha^2(\alpha - 1)(\alpha^2 - \alpha - 1), \quad c = \alpha^2(\alpha - 1)$$
とおき, 楕円曲線 E を
$$E : y^2 + (1-c)xy - by = x^3 - bx^2$$
とする.
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$: パラメータ $\alpha \in K$ を用いて楕円曲線 E を
$$E : y^2 = x(x^2 + 2(\alpha^4 + 1)x + (\alpha^4 - 1)^2)$$
とする.

今回の実験では, まず絶対値が 10^k 以下の整数 p, q, r, s をランダムに生成する. 次にパラメータ $\alpha \in K$ を

$$\alpha = \frac{p}{q} + \frac{r}{s}\sqrt{-1}$$

とおく. その α に対して, 上記のように構成した楕円曲線のねじれ部分群を計算することを 50 回行い, それらの平均時間を計算した. 結果については, $k = 5, 10, 20, 30$ に対して数値実験したものを, $\mathbb{Z}/7\mathbb{Z}$ と同型になる場合を表 1 に, $\mathbb{Z}/9\mathbb{Z}$ と同型になる場合を表 2 に, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ と同型になる場合を表 3 に記載した.

表 1　$\mathbb{Z}/7\mathbb{Z}$

k	等分多項式アルゴリズム [ms]	Doud の拡張アルゴリズム [ms]
5	163	57
10	320	103
20	731	742
30	1531	2060

表 2　$\mathbb{Z}/9\mathbb{Z}$

k	等分多項式アルゴリズム [ms]	Doud の拡張アルゴリズム [ms]
5	157	95
10	229	390
20	467	1937
30	1087	7048

表 3　$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

k	等分多項式アルゴリズム [ms]	Doud の拡張アルゴリズム [ms]
5	140	42
10	235	85
20	286	162
30	442	411

さらに $\mathbb{Z}/11\mathbb{Z}$ と同型なねじれ部分群を持つ楕円曲線に対しても数値実験を行った. この楕円曲線の構成には Schmitt, Zimmer [11, Theorem 6.18] に加えて, Kamienny, Najman [6] を参考にした. 具体的には, $K = \mathbb{Q}(\sqrt{-7})$ として, 以下のように楕円曲線 E を構成する.

- $\mathbb{Z}/11\mathbb{Z}$: b, c をパラメータ α, β を用いて,

$$b = \frac{1}{2^7\alpha}(2\alpha + \beta - 4)(\beta - 4)(\beta + 4),$$
$$c = \frac{1}{2^4\alpha}(2\alpha + \beta - 4)(\beta - 4)$$

とおき, 楕円曲線 E を

$$E : y^2 + (1 - c)xy - by = x^3 - bx^2$$

とする．ただし (α, β) は楕円曲線

$$C : V^2 = U^3 - 4U^2 + 16$$

上の K-有理点である．

今回は $C(K)$ の生成元 $(-4, -4\sqrt{-7})$ を Q とし，$kQ = (\alpha, \beta)$ として計算を行った．結果については $k = 7, 10, 13, 16$ に対して数値実験したものを表 4 に記載した．

表 4　$\mathbb{Z}/11\mathbb{Z}$

k	等分多項式アルゴリズム [ms]	Doud の拡張アルゴリズム [ms]
7	1170	186
10	3800	391
13	7720	688
16	16500	3490

5　考察

本研究では, Doud のアルゴリズムを構成するときに用いる諸定理の拡張を用いることで, 虚 2 次体上の楕円曲線のねじれ部分群を計算するアルゴリズムを構成し, 実装した．

実験結果より, $\mathbb{Z}/7\mathbb{Z}$ と $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ の場合はそれほど有意な差が見られない．だが Doud の拡張アルゴリズムの計算時間は, 前章で計算した通り, 与えられた楕円曲線の係数に依存するので, k をより大きくとると等分多項式アルゴリズムの方が速くなることが予想される．また, $\mathbb{Z}/9\mathbb{Z}$ の場合は等分多項式アルゴリズムの方がより顕著に速くなっているが, これも Doud の拡張アルゴリズムの計算時間が楕円曲線の係数の大きさに依存していることが理由の 1 つである ($\mathbb{Z}/9\mathbb{Z}$ の場合, パラメータの値をおおよそ 5 乗している)．加えて, $\mathbb{Z}/9\mathbb{Z}$ の場合, 等分多項式アルゴリズムについては, $n = 3$ に対する等分多項式の根に対応する点 P' を計算し, $3P = P'$ となる点 P を求めるという操作を行っているため, 実質 4 次の多項式の因数分解をしている．従って, 計算時間が, 因数分解を行う等分多項式の次数に依存している等分多項式アルゴリズムの方が, より顕著に速くなっている．逆に $\mathbb{Z}/11\mathbb{Z}$ の場合は, Doud の拡張アルゴリズムの方が速いが, これも等分多項式アルゴリズムの計算時間が, 因数分解を行う等分多項式の次数に依存しているからだと考えられる ($\mathbb{Z}/11\mathbb{Z}$ の場合, 因数分解する等分多項式の次数はおおよそ 60 次である)．一方係数が小さい場合, いずれの有限アーベル群に対しても Doud の拡張アルゴリズムの方が速くなっている．

従って, 係数が小さい楕円曲線や, 位数が大きい素因数を含む有限アーベル群と同型になるねじれ部分群をもつ楕円曲線に対して計算する場合に, Doud の拡張アルゴリズムの方が速くなると考えられる．

今後の課題としては, 定理 3.4 などを用いて Doud のアルゴリズムを拡張することで, 虚 2 次体以外の代数体上の楕円曲線のねじれ部分群を計算するアルゴリズムを構成できるかを検討することが挙げられる．特に実 2 次体や 3 次体の場合は定理 3.2 より, ねじれ点が整数点になるため, アルゴリズムの構成が可能であるかもしれない．

6 謝辞

本研究は, 著者が首都大学東京大学院理学研究科数理科学専攻博士前期課程在学中に, 同大学院理学研究科数理科学専攻の内田幸寛准教授の指導のもとに行ったものであります. 適切な助言を賜り, 熱心に指導してくださった内田幸寛准教授に深く感謝いたします. そしてご多忙の中, 本論文の副査を快諾していただきました内山成憲教授と横山俊一准教授に深く感謝いたします. また, 2 年間の苦楽を共にした梶野智哉氏, 樺島祐氏や, 今まで支えていただいた家族にも深く感謝いたします. そして最後に, 学生時代の 6 年間, 関わってくださったすべての方に御礼申し上げます.

参考文献

[1] Cassels, J. W. S., A note on the division values of $\wp(u)$, Math. Proc. Cambridge Philos. Soc. 45, 167–172, 1949.

[2] Chandrasekharan, K., Elliptic Functions, Springer, Berlin-Heidelberg-New York, 1985.

[3] Cremona, J. and Thongjunthug, T., The complex AGM, periods of elliptic curves over $\mathbb{C}$ and complex elliptic logarithms, J. Number Theory 133, no. 8, 2813–2841, 2013.

[4] Doud, D., A procedure to calculate torsion of elliptic curves over $\mathbb{Q}$, Manuscripta Math. 95, no. 4, 463–469, 1998.

[5] Kamienny, S., Torsion points on elliptic curves, Bull. Amer. Math. Soc, (N.S.) 23, no. 2, 371–373, 1990.

[6] Kamienny, S. and Najman, F., Torsion groups of elliptic curves over quadratic fields, Acta Arith. 152, no. 3, 291–305, 2012.

[7] Kenku, M. A. and Momose, F., Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. 109, 125–149, 1988.

[8] Lang, S., Elliptic Curves: Diophantine Analysis, Springer-Verlag, Berlin-Heidelberg-New York, 1978.

[9] Mazur, B., Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math., no. 47, 33–186, 1978.

[10] Mazur, B., Rational isogenies of prime degree, Invent. Math. 44, no. 2, 129–162, 1978.

[11] Schmitt, S. and Zimmer, H., Elliptic Curves: A Computational Approach, De Gruyter Studies in Mathematics Book 31, Walter de Gruyter & Co., Berlin, 2003.

[12] Serre, J.-P., A Cource in Arithmetic, Springer-Verlag, New York, 1973.

[13] Silverman, J., The Arithmetic of Elliptic Curves (Second Edition), Springer, Berlin-Heidelberg-New York, 2009.

[14] Washington, L., Elliptic Curves: Number Theory and Cryptography (Second Edition), Chapman and Hall/CRC, 2008.